TO AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of: **Masayuki HATANAKA**

Group Art Unit: **2131**

Serial Number: **10/069,113**

Examiner: **Taghi T. Arani**

Filed: **June 24, 2002**

Confirmation Number: **3459**

For: **RECORDING DEVICE**

Attorney Docket Number: **020233**
Customer Number: **38834**

SUBMISSION OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

August 18, 2006

Sir:

Applicants submit herewith an Appeal Brief in the above-identified U.S. patent application.

Attached please find a check in the amount of $500.00 to cover the cost for the Appeal Brief. If any additional fees are due in connection with this submission, please charge Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

Andrew G. Melick
Attorney for Appellants
Registration No. 56,868
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

AGM/tw

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

APPEAL BRIEF FOR THE APPELLANT

Ex parte Masayuki HATANAKA et al. (Applicants)

RECORDING DEVICE

Serial Number: 10/069,113

Filed: June 24, 2002

Appeal No.:

Group Art Unit: 2131

Examiner: Taghi T. Arani

Submitted by:
Andrew G. Melick
Registration No. 56,868
Attorney for Appellants

WESTERMAN, HATTORI,
DANIELS & ADRIAN, LLP
1250 Connecticut Avenue NW, Suite 700
Washington, D.C. 20036
Tel (202) 822-1100
Fax (202) 822-1111

August 18, 2006

TABLE OF CONTENTS

BRIEF ON APPEAL

I. REAL PARTY IN INTEREST

The real party in interest is **FUJITSU LIMITED, HITACH LTD AND SANYO ELECTRIC CO. LTD**, by an assignment recorded in the U. S. Patent and Trademark Office on **June 24, 2002**, at Reel **013025**, Frame **0880**.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, appellant's legal representative, or assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-5 and 13-18 are rejected under 35 U.S.C. §103(a) as being unpatentable over ***Hasebe*** (U.S. Patent No. 5,392,351) in view of ***Lang*** (U.S. Patent No. 5,191,611); and claims 6-12 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Hasebe* in view of *Lang* and further in view of ***Shear*** (U.S. Patent Application Publication No. 2001/042043).

Claims 1-18 are the subject of this appeal.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been filed subsequent to the final rejection dated January 25, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1 is the only independent claim involved in this appeal. The claimed subject matter as recited in independent claim 1 is:

1. A recording device 110 detachably attachable to a reproduction apparatus 100 reproducing and outputting encrypted content data, for receiving and recording said encrypted content data therein (*See, e.g.*, page 4, line 24 to page 5 line 30; Figs. 1 and 2); comprising:

a data input/output unit 1202 allowing external data communication (page 6, lines 19-20; Fig. 2);

a first storage unit 1412 receiving said encrypted content data from said data input/output unit for storage (page 6, lines 28-31; Fig. 2);

a user information hold unit 1530 holding first user ID data provided to identify a user of said recording device (page 7, lines 4-5; Fig. 2);

a protection information memory unit (1520 and 1540) holding protection information (page 7, lines 4-15; page 8, line 10 to page 9, line 26; Fig. 2) updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed (page 19, line 12 to page 20, line 13; Fig. 10); and

a control unit 1420 controlling an operation of said recording device (page 6, lines 27-28; Fig. 2), said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit (page 20, line 14 to page 26, line 13; Fig. 11 (S504); Fig. 12 (S602 and S604); Fig. 13 (S702 and S704); Fig. 14 (S802).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal are whether claims 1-5 and 13-18 are unpatentable over *Hasebe* in view of *Lang* under 35 U.S.C. § 103(a); and whether claims 6-12 are unpatentable over *Hasebe* in view of *Lang* and further in view of *Shear* under 35 U.S.C. §103(a).

VII. ARGUMENT

A. REJECTION UNDER 35 U.S.C. § 103(A) AS BEING UNPATENTABLE OVER *HASEBE* IN VIEW OF *LANG*

It is respectfully requested that the rejection of claims 1-5 and 13-18 under 35 U.S.C. § 103(a) as being unpatentable over *Hasebe* in view of *Lang*, be withdrawn, since *Hasebe* in view of *Lang* does not disclose each and every feature recited in the claims.

The Office Action dated January 25, 2006, finally rejects claims 1-5 and 13-18 under 35 U.S.C. § 103(a) as being obvious over *Hasebe* in view of *Lang*. It is thus the position of the Office Action that *Hasebe* in view of *Lang* teaches or suggests "a user information hold unit holding first user ID data provided to identify a user of said recording device," "a control unit controlling an operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit," "a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed," and "a recording device detachably attachable to a reproduction apparatus" as recited in claim 1.

It is respectfully submitted that *Hasebe* in view of *Lang* does not teach or suggest "a user information hold unit," "a control unit," "a protection information memory unit," and "a recording device detachably attachable to a reproduction apparatus" as recited in claim 1. Thus claim 1 cannot be obvious over *Hasebe* in view of *Lang*.

Hasebe in view of *Lang* must teach or suggest all the claim limitations of claim 1, otherwise the claim is non-obvious. MPEP § 2143.03 citing *In re Royka*, 490 F.2d 981 (CCPA 1974).

1. ***Hasebe* in view of *Lang* does not teach or suggest, "a user information hold unit holding first user ID data provided to identify a user of said recording device."**

The user information hold unit of the recording device in the claimed invention holds information corresponding to the user of the memory card in the reproduction apparatus. The user ID data in the user information hold unit 1530 is compared with user ID data 1107 registered in cell phone 100 before allowing changes to the protection information settings. (Specification, page 19, lines 13-31; Fig. 10.) User ID data can also be used to override a reproduction flag set to prohibit reproduction of content data, allowing reproduction to proceed. (Specification, page 21, lines 16-28; Fig. 11.)

The Examiner takes the position that the personal key generating unit 92 of *Hasebe* is a user information hold unit, and that the personal key generating unit generates a user's personal key using the user's personal number 91. (Office Action, January 25, 2006, page 2.) The Examiner alleges that this information identifies the user of the recording device. (Advisory Action, page 2.)

Applicants respectfully traverse the assertion that *Hasebe* in view *Lang* teaches a user information hold unit holding first user ID data provided to identify a user of said recording device.

Hasebe discloses a personal number 91 located on a user computer used by a vendor of software for creating an encryption/decryption key. On the vendor computer, the personal number is processed in the personal key generating unit 81 to create a personal key. The personal key is used in the encrypting circuit 83 to encrypt the software decrypting key 82. (Col. 3, lines 40-46; Fig. 1.) On the user computer, the personal number is processed in the personal key generating unit 92 to create a personal key. The personal key is used in the decrypting circuit 93 to decrypt the software decrypting key 94. (Col. 3, lines 47-56; Fig. 1.)

However, neither the personal number 91 nor the personal key is user information for identifying a user. The personal number is used for creating a personal key. The personal key encrypts the software decrypting key on the vendor computer and decrypts the software decrypting key on the user computer. (Col. 3, lines 40-56; Fig. 1.) The personal number is "for example, an apparatus number of a computer." (Col. 3, lines 40-43.) Thus, a software vendor prepares a software storage medium using the personal number so that use of the plain text software is limited to only the computer having the same personal number. *Hasebe* states:

> In use of the **personal number for the computer**, the execution for the computer is applied by the permission information 72 so that **only that computer can execute** the plain text software. Accordingly, the user cannot utilize a different computer even if he is authorized. Further, it is impossible to transfer such plain text software to a third-party.

(Col. 3, lines 60-66, emphasis added.) The personal number is unique to a computer and is used by a software vendor to limit use of a software storage medium to the computer from which the personal number originated.

Even if the personal number is unique to a user instead of to a computer, the personal number is not used to identify a user of the user computer. As stated above, personal number 91 is used for creating a personal key which is used by a vendor of software to encrypt a software decrypting key such that only a computer having the matching personal number can then decrypt the software decrypting key. (Col. 3, lines 40-56; Fig. 1.) The personal number is used to create an encryption/decryption key. The personal number is not used by the user computer to identify the user of the user computer.

Hasebe in view of *Lang* does not disclose "a user information hold unit holding first user ID data provided to identify a user of said recording device" as recited in claim 1. Therefore, claim 1 is patentable over *Hasebe* in view of *Lang*.

2. *Hasebe* in view of *Lang* does not teach or suggest, "a control unit controlling an operation of said recording device, said control unit referring to said protection information to restrict access to said encrypted content data held in said first storage unit."

In the present invention, the control unit 1420, controls various operations of the recording device such as reproduction of content data, erasure of content data, transfer of content data. Control unit 1420 controls these various operations by referring to the protection information. Protection information is referred to before proceeding to decryption of the

encrypted data. (Fig. 11, S504; Fig. 12, S602 and S604; Fig. 13, S702 and S704; Fig. 14, S802.) For example, if the content reproduction flag in the protection information memory unit is set in a status allowing content data to be reproduced, then controller 1420 allows the decryption unit 1416 to decrypt the encrypted data. (Specification, page 21, lines 2-15; Fig. 11.) Otherwise, if the content reproduction flag is set in a status such that content data is not to be reproduced, then controller 1420 proceeds on a different processing path and may disallow reproduction of the content data. (Specification, page 21, lines 16-31; Fig. 11.)

The Examiner takes the position that the decrypting circuit 93 of *Hasebe* is a control unit, and that the decrypting circuit decrypts the permission information 72 from the software storage medium 71 based on the personal key 81. (Office Action, January 25, 2006, page 2.)

Applicants respectfully submit that the decrypting circuit 93 of *Hasebe* does not control the operation of the recording device, thus *Hasebe* does not disclose:

> a control unit controlling the operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit

as recited in claim 1.

The decrypting circuit 93 of *Hasebe* decrypts permission information 72 using the personal key generated by the personal key generating unit. The decrypting circuit does not refer to information for restricting access to the encrypted permission information. In other words, the decrypting circuit does not determine whether certain conditions are met before decryption proceeds. The decryption circuit attempts decryption without referring to protection information

that may restrict access. If the personal key is incorrect then the decryption attempted by the decryption circuit fails. The decryption circuit does not refer to protection information before attempting to decrypt the data.

Hasebe does not disclose "a control unit controlling the operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit" as recited in claim 1. Therefore, claim 1 is patentable over *Hasebe* in view of *Lang*.

3. *Hasebe* in view of *Lang* does not teach or suggest, "a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed."

Protection information is information such as whether or not additional recording is allowed on the recording device and whether or not data is erasable on the recording device (specification, page 8, Table 1), and whether or not specific content is reproducible or erasable (specification, page 9, Table 2). Protection information is set and updated by the user. (Specification, page 19, line 24 to page 20, line 2; Fig. 10) Once the recording device determines that the externally provided user information matches the first user ID stored in the recording device, the user is allowed to update the protection information. (Specification, page 19, lines 17-31; Fig. 10.)

The Examiner takes the position that permission information 13 of *Hasebe* is protection information as recited in claim 1. (Office Action, January 25, 2006, page 3, citing *Hasebe*, col. 5, lines 40-45.) The Examiner acknowledges that *Hasebe* does not disclose that protection information is updatable in response to a result of comparing externally provided user information with said first user ID data. (Office Action, page 3.) The Examiner cites *Lang* at col. 12, lines 36-58 for disclosing such a feature. This passage states a procedure for limiting and controlling user privileges to information.

Applicants respectfully submit that neither *Hasebe* nor *Lang*, taken individually or in combination, disclose:

> a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed

as recited in claim 1.

Permission information 13 in *Hasebe* is the encrypted data decrypting key. "[P]ermission information 13 incorporates encrypted data for decrypting the encrypted software." (Col. 5, lines 41-44.) Permission information 13 is generated by the vendor computer by encrypting the software decrypting key. (Col. 5, lines 40-45; Figs. 1-3.) Permission information 13 is not information such as whether or not additional recording is allowed, whether or not data is erasable, and whether or not data is reproducible.

Furthermore, *Lang* does not disclose that protection information is updatable in response to a result of comparing externally provided user information with the first user ID data, as externally provided. *Lang* at col. 12, lines 36-58, cited by the Examiner for disclosing this feature, states a procedure for an information provider to limit and control user privileges to information. The procedure first states that users authorized by the information provider are given a specific number of information retrievals. Once the specific number of retrievals has been reached, the user must renew or update privileges to information. To renew user privileges, the user must request renewal. Then the information provider gives the user an updated access code. In *Lang*, information providers protect information by restricting access to users to a specific number of information retrievals. In the present claimed invention, a user that corresponds to the first user ID data on the recording device has control of the protection of information on the recording device.

Neither *Hasebe* nor *Lang* disclose a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with the first user ID data, as externally provided. Therefore, claim 1 is patentable over *Hasebe* in view of *Lang*.

4. *Hasebe* in view of *Lang* does not teach or suggest, "a recording device detachably attachable to a reproduction apparatus."

The present invention relates to a memory card that is accommodated by a recording device. The memory card has a data input/output unit 1202, a first storage unit 1412, a user

information hold unit 1530, a protection information memory unit (1520 and 1540), and a control unit 1420. (Fig. 2.) The memory card 110 is detachably attachable to cell phone 100. (Specification, page 5, lines 18-20.)

Applicants respectfully submit that *Hasebe* in view of *Lang* does not disclose "a recording device detachably attachable to a reproduction apparatus" as recited in claim 1.

Hasebe does not disclose a circuit having the above elements in the detachably attachable storage media. The personal key generating unit 92 and the decrypting circuit 93 are cited by the Examiner as the "user information hold unit" and the "control unit," respectively. (Office Action, page 3.) *Hasebe* discloses that personal number 91, personal key generating unit 92 and decrypting circuit 93 are included in the user computer. (Col. 3, lines 23-26.) In addition, the Examiner cites *Hasebe* at col. 3, lines 54-56 for disclosing the "data input/output unit" and the "first storage unit." *Hasebe* at col. 3, lines 54-56 discusses the storage of the user computer, not the detachably attachable storage medium.

Therefore, *Hasebe* in view of *Lang* does not teach a recording device detachably attachable to a reproduction apparatus as recited in claim 1.

B. REJECTION UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER *HASEBE* IN VIEW OF *LANG* AND FURTHER IN VIEW OF *SHEAR*

It is respectfully requested that the rejection of claims 6-12 under 35 U.S.C. § 103(a) as being unpatentable over *Hasebe* in view of *Lang* and further in view of *Shear*, be withdrawn. *Shear* fails to disclose the features that are not disclosed in *Hasebe* and *Lang* as pointed out above. Claims 6-12 depend, either directly or indirectly, from claim 1. Thus, Applicants submit that claims 6-12 are patentable over *Hasebe* in view of *Lang* and further in view of *Shear*.

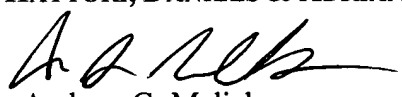
VIII. CONCLUSION

In view of the above remarks, Applicants respectfully submit that the rejection of claims 1-5 and 13-18 under 35 U.S.C. § 103(a) as being unpatentable over *Hasebe* in view of *Lang* and claims 6-12 under 35 U.S.C. § 103(a) as being unpatentable over *Hasebe* in view of *Lang* and further in view of *Shear* should be withdrawn.

If this paper is not timely filed, Applicants hereby petition for an appropriate extension of time. The fee for any such extension may be charged to Deposit Account No. 50-2866, along with any other additional fees that may be required with respect to this paper.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP



Andrew G. Melick
Attorney for Appellants
Registration No. 56,868
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

AGM/tw

IX. CLAIMS APPENDIX

1. A recording device detachably attachable to a reproduction apparatus reproducing and outputting encrypted content data, for receiving and recording said encrypted content data therein, comprising:

a data input/output unit allowing external data communication;

a first storage unit receiving said encrypted content data from said data input/output unit for storage;

a user information hold unit holding first user ID data provided to identify a user of said recording device;

a protection information memory unit holding protection information updatable in response to a result of comparing externally provided user information with said first user ID data, as externally instructed; and

a control unit controlling an operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit.

2. The device of claim 1, wherein said control unit allows said user ID data to be changed when externally provided user information and said first user ID data match.

3. The device of claim 2, wherein said control unit allows said protection information to be added and said user ID data to be added when said user information hold unit does not have said first user ID data registered therein.

4. The device of claim 1, wherein:

said protection information memory unit includes a first protection information memory unit holding first protection information included in said protection information for restriction on access to said recording device itself; and

said control unit is driven by said first protection information to prohibit additionally recording new encrypted content data in said first storage unit.

5. The device of claim 1, wherein:

said protection information memory unit includes a first protection information memory unit holding first protection information included in said protection information for restriction on access to said recording device itself; and

said control unit is driven by said first protection information to prohibit erasing new encrypted content data in said first storage unit.

6. The device of claim 5, wherein:

said protection information memory unit further includes a second protection information memory unit holding second protection information included in said protection information for restriction on access for each said encrypted content data; and

said control unit is driven by said first and second protection information to prohibit erasing encrypted content data held in said first storage unit and corresponding to said second protection information.

7. The device of claim 1, wherein:

said protection information memory unit further includes a second protection information memory unit holding second protection information included in said protection information for restriction on access for each said encrypted content data; and

said control unit is driven by said second protection information to prohibit erasing encrypted content data held in said first storage unit and corresponding to said second protection information.

8. The device of claim 6, wherein when an external instruction is received to effect an operation to reproduce said encrypted content data, said control unit controls said first storage unit and is driven by said second protection information to prohibit providing said data input/output unit with encrypted content data held in said first storage unit.

9. The device of claim 8, wherein when externally provided user information and said first user ID data match said control unit controls said first storage unit and is driven by said second protection information to prohibit providing said data input/output unit with encrypted content data held in said first storage unit.

10. The device of claim 8, wherein when said user information hold unit does not have said first user ID data registered therein said control unit controls said first storage unit and is driven by said second protection information to prohibit providing said data input/output unit with encrypted content data held in said first storage unit.

11. The device of claim 6, wherein when externally provided user information and said first user ID data match said control unit permits rewriting at least one of said first and second protection information.

12. The device of claim 6, wherein when said user information hold unit does not have said first user ID data registered therein said control unit permits rewriting at least one of said first and second protection information.

13. The device of claim 1, further comprising a second storage unit (1500) holding license information data corresponding to said encrypted content data, respectively, and required for reproducing said encrypted content data, wherein when an external instruction is received to transfer said encrypted content data held in said first storage unit, said control unit is driven by a

result of comparing second user ID data externally provided for said reproduction apparatus with said first user ID data held in said user information hold unit, to control said second storage unit to provide said license information data to said data input/output unit.

14. The device of claim 1, further comprising a second storage unit holding license information data corresponding to said encrypted content data, respectively, and required for reproducing said encrypted content data, said license information each including content user ID data corresponding for each said encrypted content data, wherein an external instruction is received to transfer said encrypted content data held in said first storage unit, said control unit is driven by a result of comparing second user ID data externally provided for said reproduction apparatus, said first user ID data held in said user information hold unit and said content user ID data with each other, to control said second storage unit to provide said data input/output unit with said license information data for each said encrypted content data.

15. The device of claim 14, wherein said control unit is driven by a result of comparing second user ID data externally provided for said reproduction apparatus with said first user ID data held in said user information hold unit, to permit changing said content user ID data.

16. The device of claim 14, wherein said content user ID data is said first user ID data held in said user information hold unit when said encrypted content data corresponding thereto is distributed.

17. The device of claim 16, wherein said control unit is driven by a result of comparing second user ID data externally provided for said reproduction apparatus with said first user ID data held in said user information hold unit, to permit changing said content user ID data.

18. The device of claim 1, wherein:

said first storage unit is semiconductor memory; and

said recording device is a memory card.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.